RODO – a może mnie to nie dotyczy…?

Tomasz Wyrozumski
BMS Creative

To już trzeci i ostatni artykuł z cyklu „RODO". No cóż, 25 maja coraz bliżej, a my? Ciągle jeszcze w lesie? Niby wiemy już w czym rzecz, ale może rozporządzenie wcale nas nie dotyczy? Może nasza firma nie jest administratorem danych osobowych? To prawda, mamy „zapisane" kontakty do pracowników naszych kontrahentów, ale czy je przetwarzamy? Dzwonimy, wysyłamy maile i to wszystko. O co więc tyle hałasu?

Niestety, rozporządzenie nie pozostawia tu żadnych wątpliwości. Zgodnie z nim: *„przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.*

A zatem nawet samo przechowywanie danych osobowych jest już ich przetwarzaniem i to powinno ostatecznie rozwiać wątpliwości niektórych czytelników. Na dodatek, zgodnie z rozporządzeniem, każde przetwarzanie musi mieć swoją podstawę prawną. Może nią być np. przepis prawa – przykładowo, jeśli wystawiamy faktury osobom fizycznym, jesteśmy zobligowani do przechowywania ich kopii, niezależnie od tego, czy naszym klientom się to podoba, czy nie. W innych przypadkach podstawę może stanowić umowa, gdy do jej wykonania przetwarzanie danych osobowych zainteresowanego jest konieczne, albo też wreszcie indywidualna zgoda. I tu bardzo ważna uwaga: zgodna nie może być domyślna. Jeżeli więc miałaby zostać wyrażona poprzez wypełnienie formularza na portalu internetowym, to pole „Wyrażam zgodę" nie może być z góry zaznaczone – wypełniającemu należy zapewnić komfort w pełni świadomego podjęcia decyzji.

Idąc dalej, przetwarzanie danych osobowych musi mieć jasno określony cel i tego, a nie innego celu powinna dotyczyć ewentualna zgoda. Gdy celów jest wiele, powinno też być wiele zgód. Jeżeli więc np. zezwolimy, aby warsztat samochodowy przetwarzał nasze dane po to, by informować nas o okresowych przeglądach, to pobieranie i analizowanie informacji o zużyciu paliwa z komputerów pokładowych naszych samochodów wymagać już będzie odrębnej zgody. Oczywiście nie ma przeszkód, by kilka celów ująć razem, łącząc je spójnikiem „lub" – ryzykujemy jedynie, że któryś nie przypadnie do gustu zainteresowanemu, co skutkować będzie brakiem zgody na każdy z nich. Pamiętajmy o prawie Augusta De Morgana: zaprzeczenie alternatywy jest równoważne koniunkcji zaprzeczeń!

Całkiem odrębną podstawę może stanowić *prawnie uzasadniony interes administratora*. Ocenę, czy konkretny rodzaj przetwarzania wyczerpuje jego znamiona, czy też nie, pozostawiamy czytelnikom, odsyłając ich do szczegółów rozporządzenia. Niemniej jednak warto przytoczyć tu stwierdzenie, ważne dla bardzo wielu firm: *za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego*. Tak więc marketing bezpośredni nie wymaga specjalnej zgody osoby, do której jest adresowany, choć z drugiej strony osobie takiej rozporządzenie przyznaje prawo sprzeciwu wobec jego stosowania, a nawet prawo do żądania usunięcia jej danych z bazy (więcej na ten temat w dalszej części artykułu).

Dodatkowo, o wszystkim tym należy zainteresowanego *jasno i odrębnie od wszelkich innych informacji* powiadomić *najpóźniej przy okazji pierwszej komunikacji*.

Z powyższych rozważań płynie oczywisty wniosek: nad danymi osobowymi musimy mieć kontrolę. Jeżeli ją bowiem utracimy, jeśli dane „wyciekną", to nie będziemy mogli zagwarantować, że przetwarzane są one w celu zgodnym z podstawą prawną przetwarzania.

Rozporządzenie nie określa, w jaki dokładnie sposób powinny być zabezpieczane zbiory danych, pozostawiając w tej kwestii decyzję ich administratorom. Z jednej strony to dobrze, ponieważ nikt nikomu nie narzuca bezsensownych procedur, z drugiej jednak – cała odpowiedzialność spada właśnie na administratora i nie wystarczy powiedzieć: „zrobiłem to zgodnie z przepisami, a że w przepisach czegoś nie przewidziano, to już nie moja wina". Oczywiście, tzw. *dane wrażliwe* (np. dotyczące stanu zdrowia) powinny być przetwarzane z zachowaniem znacznie większej ostrożności, niż, powiedzmy, informacje o preferencjach odnoście marek samochodów. Tym niemniej jednak, każde dane osobowe winny być należycie chronione.

Jak to osiągnąć w praktyce? Przede wszystkim trzeba mieć pełną jasność, gdzie się te dane znajdują. Niby oczywiste, lecz w istocie wcale nie takie proste, zwłaszcza jeśli firma nie wykorzystuje jednego, zintegrowanego systemu informatycznego, lecz posiada wiele baz danych rozproszonych po różnych komputerach: coś tam jest w programie do fakturowania, coś w książkach adresowych Outlooka u poszczególnych handlowców, coś znów w podręcznych Excelach, służących do rozmaitych celów. Czyż nie tak? A kontakty w telefonach? Częstokroć nawet niezabezpieczonych kodem PIN… Przecież wystarczy, że ktoś zgubi taki telefon, albo notebooka, na który użytkownik Jasio loguje się hasłem „jasio" i już kłopot gotowy. Bywa też, że doskonale zabezpieczona baza danych spoczywa na dysku komputera, który wcale nie znajduje się w odpowiednio strzeżonym pomieszczeniu, lecz w ogólnodostępnym pokoju, z którego po prostu łatwo go ukraść. A może przechowywana jest w tzw. chmurze? To bardzo modne słowo, jednakże warto sprawdzić, co oznacza ono w rzeczywistości – profesjonalną serwerownię, czy też może piwnicę w bloku mieszkalnym, zamkniętą w najlepszym razie na solidną kłódkę?

Niestety, sankcje za niefrasobliwość mogą być dotkliwe – nawet do 20 mln EUR… No dobrze, nie straszmy – po pierwsze, kara nie może przekroczyć 4% całkowitego rocznego obrotu przedsiębiorstwa, po drugie, przy jej nakładaniu rozporządzenie nakazuje zważenie wszelkich okoliczności zdarzenia i określenie jej wysokości proporcjonalnie do szeroko rozumianego charakteru naruszenia, w tym jego umyślności. Jest to oczywiście jakaś pociecha, ale lepiej po prostu się nie narażać.

Warto też pamiętać, że osoba, której dane przetwarzamy, w bardzo wielu sytuacjach może się temu sprzeciwić. Wtedy powinniśmy zaprzestać przetwarzania jej danych, czyli, krótko mówiąc, usunąć je z bazy. Usunąć? Łatwo powiedzieć! Z technicznego punktu widzenia wcale nie jest to jednak banalne. Relacyjna baza danych (a z takimi właśnie mamy na ogół do czynienia w systemach informatycznych) nie pozwoli tak po prostu skasować rekordu, który jest powiązany z innymi – np. z notatkami, ofertami itp. Nie wdając się w szczegółowe rozważania na temat tego, co i kiedy da się zrobić, a czego na pewno nie, skonstatujemy tylko, że praktycznie jedyną sensowną metodą usunięcia danych osobowych z systemu informatycznego jest tzw. anonimizacja. Sprowadza się ona do tego, że, co prawda, wspomniane notatki, bądź oferty pozostaną, to jednak nie będzie expressis verbis zapisane, kogo dokładnie dotyczą. Edytujemy więc dane określonego pracownika naszego kontrahenta i w miejsce imienia i nazwiska wpisujemy gwiazdki. Proste? Niestety nie… Nie ma bowiem żadnej gwarancji, że wszystkie dane w systemie przechowywane są na tzw. relacjach, a więc, że owo imię i nazwisko już nigdzie się nie pojawi. Co więcej, w bardzo wielu przypadkach jest dokładnie odwrotnie, a to oznacza, że jedyną gwarancją poprawnej anonimizacji jest użycie

odpowiedniej funkcji udostępnionej przez producenta oprogramowania – oczywiście przy założeniu, że świadom nowych obowiązków, funkcję taką udostępnił.

Rozporządzenie zaleca też korzystanie z *pseudonimizacji* danych osobowych. Chodzi tu o to, by „na co dzień" przetwarzać dane w sposób uniemożliwiający ustalenie, kogo one dotyczą, a więc np. zaszyfrować je przy użyciu klucza przechowywanego oddzielnie i dostępnego tylko dla wybranych pracowników. Choć nie zawsze, jednak w niektórych sytuacjach, np. dla celów analiz statystycznych, jest to całkiem wystarczające, a znakomicie redukuje prawdopodobieństwo „wycieku", umożliwiając jednocześnie odzyskanie źródłowej informacji, jeśli tylko zajdzie taka potrzeba.

Wiele uwagi poświęcono ponadto w rozporządzeniu *profilowaniu,* które polega na *dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby*. Może nie jest to napisane wprost, lecz de facto profilowanie wymaga na ogół odrębnej zgody zainteresowanego, i to w kontekście celu, jakiemu służy.

Jeśli komuś natomiast spędzają sen z powiek pogłoski o konieczności prowadzenia ściśle określonych rejestrów czynności przetwarzania danych osobowych, to pewnym pocieszeniem może być fakt, iż przepis ten dotyczy wyłącznie firm zatrudniających co najmniej 250 pracowników. Tak więc jedynie niektórym czytelnikom zalecamy zapoznanie się z art. 30 rozporządzenia.

I jeszcze jedno: komunikacja pomiędzy administratorem danych osobowych, a osobą, której dane te dotyczą, powinna być prowadzona językiem jasnym, prostym i zrozumiałym. Niby oczywiste, ale wszyscy wiemy, jak to na ogół w praktyce wygląda, więc może i dobrze, że Parlament Europejski i Rada Unii postanowiły zwrócić na to szczególną uwagę.

Podsumowując, co w praktyce należy koniecznie zrobić? Spróbujmy ująć to w punktach:

a) przeszkolić pracowników w zakresie obowiązków wynikających z rozporządzenia;

b) zinwentaryzować posiadane bazy danych osobowych i w miarę możliwości zredukować ich ilość do niezbędnego minimum – najlepiej do jednej, w ramach zintegrowanego systemu informatycznego;

c) zabezpieczyć bazy (fizycznie i logicznie) w sposób adekwatny do charakteru przetwarzanych danych;

d) jeśli przetwarzanie nie wynika z przepisów prawa, zawartych umów, bądź też prawnie uzasadnionego interesu administratora – uzyskać zgody od osób, których dane podlegają przetwarzaniu, uwzględniając przy tym cele przetwarzania;

e) dostosować umowy, formularze na stronach www itp. do wymogów rozporządzenia;

f) usunąć (zanonimizować) dane tych osób, które nie wyraziły zgody, bądź też skutecznie sprzeciwiają się przetwarzaniu ich danych.

Na koniec wypada zaznaczyć, że zarówno powyższa lista, jak i cały artykuł, powinny być traktowane jedynie jako zbiór wskazówek dla administratorów baz danych osobowych. W żadnym razie nie wyczerpują one tematu i nie odnoszą się do zagadnień szczegółowych, lecz raczej, wobec ogromnej ilości wszechobecnych komentarzy prawników, stanowią spojrzenie z nieco innej perspektywy – z pozycji informatyka, co może być istotne o tyle, że w końcu o przetwarzanie danych w tym wszystkim chodzi.